

### Claims

1. A method for generating and transmitting a  
5 data set between two parties H and B comprising the steps  
of

a) providing a cover data set (CD) corre-  
sponding to the data set to be transmitted,

b) generating a stego data set (SD) of said  
10 cover data set (CD) by embedding at least one digital wa-  
termark in said cover data set (CD), wherein said water-  
mark is encoded using at least one key of an asymmetric  
cryptographic key pair ( $ps_H$ ,  $vs_H$ ) of H, said key pair  
comprising a secret private key ( $ps_H$ ) and a known public  
15 key ( $vs_H$ ) derived therefrom,

c) encrypting said stego data set (SD) using  
said key pair ( $ps_H$ ,  $vs_H$ ) of H,

d) transmitting said encrypted stego data set  
from said party H to said party B.

20

2. The method of claim 1, wherein said step  
c) comprises

generating a mask message ( $B||SN$ ),

generating a signature ( $DSSMR_G(ps_H, B||SN)$ )

25 of said mask message ( $B||SN$ ) using said secret private  
key ( $ps_H$ ), and

using said signature of said mask message for  
seeding an encryption algorithm for said stego data set  
(SD).

30

3. The method of claim 2 wherein said signa-  
ture ( $DSSMR_G(ps_H, B||SN)$ ) of said mask message ( $B||SN$ )  
is transmitted from H to B.

35

4. The method of one of the claims 2 or 3  
wherein said encryption algorithm comprises the step of  
calculating the Fourier transform of said stego data set

26.08.99

(SD), modifying the phase components of the Fourier transform using a pseudo-random pattern seeded by said signature ( $DSSMR_G(ps_H, B||SN)$ ) of said mask message ( $B||SN$ ) and calculating the inverse Fourier transform for generating the encrypted stego data set.

5. The method of one of the preceding claims wherein said key pair ( $ps_H, vs_H$ ) of H is an elliptic curve key pair.

10

6. The method of one of the preceding claims wherein said step b) comprises the step of generating at least one watermark of a first type, wherein said watermark of a first type is encoded using said private key ( $ps_H$ ) of H.

15

7. The method of claim 6 wherein said watermark of a first type is encoded using a hash value ( $crh(ps_H)$ ) of said private key ( $ps_H$ ) and can be decoded by using said hash value ( $crh(ps_H)$ ).

20

8. The method of claim 6 wherein said watermark of a first type is encoded using a hash value ( $crh(OAD_{CD})$ ) of a signature ( $OAD_{CD}$ ) generated using said private key ( $ps_H$ ).

25

9. The method of one of the preceding claims wherein said step b) further comprises the step of generating at least one watermark of a second type, wherein said watermark of a second type comprises a payload ( $pc_H[AM]$ ) derived from the Fourier transform of said cover data (CD).

30

10. The method of one of the preceding claims wherein said step b) comprises the steps of:

35

i) providing a message ( $s_1, s_2, \dots, s_M$ ) to be transmitted in said at least one watermark, said message consisting of a plurality of symbols,

ii) providing a pseudo random generator  
5 seeded with a seed value derived from a key of said key pair ( $ps_H, vs_H$ ) of H or a hash value thereof,

iii) encoding said message using values from said pseudo random generator

iv) using the said encoded message ( $m$ ) for  
10 embedding said watermark.

11. The method of claim 10 wherein said step iii) comprises:

for each of said symbols ( $s_i$ ), generating a  
15 pseudo random sequence of numbers ( $v_1, v_2, \dots$ ) by a said pseudo random generator,

using the value of each said symbols ( $s_i$ ) for selecting a sub-sequence within said pseudo random sequence for forming a symbol vector ( $r_i$ ), and

20 adding said symbol vectors ( $r_i$ ) to generate said encoded message ( $m$ ).

12. The method of claim 11 comprising the following steps for decoding said message:

25 extracting a read-out message ( $m'$ ) from said watermark, said read-out message being a vector having the same length, if erased elements are replaced by zero, as said symbol vectors ( $r_i$ ),

generating all possible values of said symbol  
30 vectors ( $r_i$ ) using said pseudo random generator seeded with said seed, and

calculating the cross-correlation between said pseudo random sequences of numbers ( $v_1, v_2, \dots$ ) and said read-out message ( $m'$ ) for retrieving said symbols  
35 ( $s_i$ ).

13. The method of claim 10 wherein said step  
iii) comprises:

for each bit ( $b_j$ ) of said symbol sequence  
( $s_1, s_2, \dots, s_M$ ), deriving pseudo random vectors ( $r_j^*$ )  
5 having elements 1 or -1 from a said pseudo random genera-  
tor, which pseudo random generator preferably generates  
m-sequences or Gold codes, and

depending on the value of said bit ( $b_j$ ), mul-  
tiplying said pseudo random vector ( $r_j^*$ ) with +1 or -1 to  
10 generate a modified pseudo random vector, and adding said  
modified pseudo random vectors to generate an encoded  
message ( $m$ ).

14. The method of claim 13 comprising the  
15 following steps for decoding said message:

extracting a read-out message ( $m'$ ) from said  
watermark,

deriving said pseudo random vectors ( $r_j^*$ )  
from said pseudo random generator seeded with a said  
20 seed, and

calculating the cross correlation between  
each of said pseudo random vectors ( $r_j^*$ ) and said read-  
out message ( $m'$ ) for retrieving the corresponding bit  
( $b_j$ ) of the said symbol sequence ( $s_1, s_2, \dots, s_M$ ).

25

15. The method of one of the claims 10 - 14  
wherein the position of components to be modulated by  
each value of the encoded message ( $m$ ) is given by a  
pseudo random generator seeded by a key known by both H  
30 and B.

16. The method of one of the preceding claims  
comprising the step of encoding a message for being em-  
bedded in said watermark by using symbol based Reed Solo-  
35 mon codes as error control codes.

17. The method of one of the preceding claims wherein said step b) further comprises the step of calculating a logarithm of said cover data set (CD) before embedding said watermark for embedding said watermark in a perceptually flat domain.

18. A method for generating a stego data set (SD) from a cover data set (CD) comprising the steps of:  
generating at least one message ( $ID_{CD}$ ),  
digitally signing said message ( $ID_{CD}$ ) using an asymmetric cryptographic key pair ( $p_H$ ,  $v_H$ ) and a signature generating algorithm (DSSMR) with message recovery for generating a digital signature ( $OAD_{CD}$ ), and  
generating said stego data set (SD) of said cover data set (CD) by generating at least one digital watermark, wherein said digital signature ( $OAD_{CD}$ ) is used for deriving a seed for generating said watermark.

19. A method for embedding a watermark in a cover data set for generating a stego data set, comprising the steps of  
calculating at least some magnitude Fourier components (MC) of said cover data set (CD),  
applying an authentication function (AF) for generating a value (AM) derived from said Fourier components (MC),  
ciphering said value (AM) using a secret key ( $pc_H$ ) of an asymmetric key pair ( $pc_H$ ,  $vc_H$ ) for generating a ciphered message, and  
embedding said ciphered message as a payload in a public watermark.

20. A method for verifying the originality of a possibly modified stego data set generated with the method of claim 19 comprising the step of reading said value (AM) by decoding said ciphered message using the

public key of said key pair and comparing said magnitude Fourier components to said stego data set.

21. Method for generating and transmitting a data set between two parties H and B, comprising the steps of

providing a cover data set (CD) corresponding to the data set to be transmitted,

generating a stego data set (SD) of said cover data set (CI) at a party H by generating at least one digital watermark in said cover data set (CD),

transmitting a hash value of said stego data set (SD) to a registration party (O), and

permanently storing certification data (CCD) at said registration party (O), said certification data comprising said hash value of said stego data set (SI), a digital time stamp (TVP) and information designating said party H.

22. The method of claim 21 further comprising the steps of generating a digital signature of said certification data (CCD) using an asymmetric cryptographic key pair ( $ps_0$ ,  $vs_0$ ) of said registration party (O), transmitting said certification data (CCD) and said digital signature to said party H, and verifying said digital signature at said party H by using a public key ( $vs_0$ ) of said key pair of said registration party.

30